VZCZCXRO8928
PP RUEHFL RUEHNP
DE RUEHRO #0095/01 0231400
ZNY CCCCC ZZH
P 231400Z JAN 08
FM AMEMBASSY ROME
TO RUEHC/SECSTATE WASHDC PRIORITY 9710
INFO RUEHFL/AMCONSUL FLORENCE PRIORITY 2862
RUEHMIL/AMCONSUL MILAN PRIORITY 9202
RUEHNP/AMCONSUL NAPLES PRIORITY 3012
RUEAIIA/CIA WASHDC PRIORITY
RUEAHLC/DEPT OF HOMELAND SECURITY WASHINGTON DC PRIORITY
RHMCSUU/FBI WASHINGTON DC PRIORITY

C O N F I D E N T I A L SECTION 01 OF 07 ROME 000095

SIPDIS

SIPDIS

S/CT FOR KEN MCKUNE

E.O. 12958: DECL: 12/09/2017
TAGS: KVPR PTER PREL PGOV PINR CVIS ASEC KHLS IT
SUBJECT: ITALY: RESPONSE TO REQUEST FOR INFORMATION ON HOST GOVERNMENT PRACTICES - INFORMATION COLLECTION, SCREENING, AND SHARING

REF: STATE 133921

Classified By: A/POL M/C Jonathan R. Cohen, for reasons 1.4 (b) and (d)

¶1. (SBU) The following are Embassy Rome's answers to the questionnaire on host government information collection, screening and sharing practices contained in Reftel.

¶2. (SBU) Section A: Watchlisting

Question: If host government maintains a "watchlist," how many records does the watchlist contain, and how many are terrorist-related?

Answer: The Government of Italy (GOI) does not maintain a consolidated terrorist watchlist shared by all agencies. However, the Ministry of the Interior's National Police (Polizia di Stato) maintain a watchlist/database that includes names associated with criminal and terrorist activities. The National Gendarmerie (Carabinieri), Financial Police (Guardia di Finanza), Border Police and others input data into the National Police database. This information generally includes prior arrests, convictions, wanted persons, including those subjects of investigations that have reached the point of an active judicial investigation (under the authority of a prosecutor). In the case of active terrorism investigations, the investigating authority is mandated to disseminate the information to the appropriate law enforcement authorities. It is not known how many entries in the database are terrorist-related, as some listings may fall under multiple headings, not all of which fit the definition of terrorism. Border control officials also use the Schengen database, which serves to identify fugitives or individuals who are not admissible to the Schengen area.

Q: Which ministry or office maintains the watchlist?

A: National Police (Ministry of the Interior).

¶3. (SBU) Section B: Traveler Information Collection

Q: What are the country's policies (legislation, mandates, etc.) on collecting information from travelers arriving in the country?

A: Non-EU citizens arriving in Italian territory have to fill

out a series of information forms at customs and police controls. Non-EU citizens are also subject to screening for admission to the Schengen area (see below).

Q: Are there different policies for air, sea, and land entry and for domestic flights?

A: There are no substantial differences regarding data collected at different ports of entry (terrestrial, maritime or airports). However, as a result of the events of 9/11, Schengen regulations state that all airlines flying into a Schengen country must communicate to border police authorities the following data on passengers obtained during the check-in phase: a) number, type and expiry date of travel ID; b) Citizenship; c) Full name; d) Date and place of birth; e) Point of entry into Italy; f) Flight number, date of departure and arrival; g) Departure time and duration of the flight; h) Total number of passengers on the flight; and i) First point of embarkation.

Q: Who collects traveler information?

A: Depending upon the point of entry, either the operators of the transport service collect the information and pass it to administrative or police authorities, or the administrative or police authorities collect it themselves and enter it into the Schengen database.

Q: What are the policies of the collecting agency to share that information with foreign governments?

A: Private data collected by Italian border or police authorities, as long as it is not covered by state secrets,

can be exchanged with police authorities of other EU member States, of other bordering States, or of States with which specific exchange agreements have been reached, for legitimate law enforcement purposes.

Q: If applicable, have advance passenger information systems (APIS), interactive advanced passenger information systems (IAPIS), or electronic travel authority systems been effective at detecting other national security threats, such as wanted criminals?

A: Significant experience regarding the application of the system provided under EU Directive 2004/82/Ce is lacking and thus any evaluation is premature.

¶4. (SBU) Section C. Border Control and Screening

Q: Does the host government employ software to screen travelers of security interest?

A: The Government uses the Italian Ministry of Interior National Police Data Bank to screen travelers of security interest.

Q: Are all travelers tracked electronically, or only non-host-country nationals? What is the frequency of travelers being "waived through" because they hold up what appears to be an appropriate document, but whose information is not actually recorded electronically? What is the estimated percentage of non-recorded crossings, entries and exits?

A: Border officials use standard EU and Schengen guidelines for reviewing and recording travel document information. There is no European electronic entry-exit tracking system.

Q: Do host government border control officials have the authority to use other criminal data when making decisions on who can enter the country? If so, please describe this

authority (legislation, mandates, etc.)

A: They do have such authority under national and EU legislation, and border control officials also use the Schengen database, which serves to identify fugitives or other individuals who are not admissible to the Schengen area.

Q: What are the host government's policies on questioning, detaining and denying entry to individuals presenting themselves at a point of entry into the country? Which agency would question, detain, or deny entry?

A: The Border Police or Financial/Customs Police would have that responsibility, depending on the circumstances and the port of entry. Specific attention is paid to travelers from certain areas of interest that may pose a risk for human trafficking/illegal immigration, terrorism or drug trafficking.

Q: How well does information sharing function within the host government, e.g., if there is a determination that someone with a valid host-government visa is later identified with terrorism, how is this communicated and resolved internally?

A: Information sharing functions well within the government. The National Police (Polizia di Stato), Gendarmerie (Carabinieri), Financial Police (Guardia di Finanza), Border Police and others input data into the National Police computer database. This information generally includes prior arrests, convictions, wanted persons, including those subjects of investigations that have reached the point of an active judicial investigation (under the authority of a prosecutor). A judicial investigation is a mandatory act upon discovery of any crime by any law enforcement agency. The prosecutor (judicial authority) is responsible for overseeing the criminal investigation as well as prosecution. The prosecutor directs the appropriate law enforcement agency to proceed with the investigation. Therefore, using the example provided in the question, if a determination was made that someone with a valid host-government visa was later identified with terrorism, the investigating law enforcement agency would be mandated to immediately inform the judicial

authority and the prosecutor would then disseminate the information to the appropriate law enforcement authority and resolve any jurisdictional issues.

¶5. (SBU) Section D: Biometric Collection

Q: Are biometric systems integrated for all active POEs? What are the systems and models used?

A: Biometric systems are not yet in place for points of entry but Italy has plans to implement a biometric system in order to comply with the Schengen Agreement by 2008. The model currently being developed is "Italdata SPAID500." By 2008 it is likely that digital fingerprint systems will be in place at all points of entry. The Italian government is looking at an E-Passport reader called "3M-IT." The name of the program for the distribution and operation of this technology is SIF. (See also Section J below)

Q: Are all passengers screened for the biometric or does the host government target a specific population for collection (i.e. host country nationals)? Do the biometric collection systems look for a one to one comparison (ensure the biometric presented matches the one stored on the e-Passport) or one to many comparison (checking the biometric presented against a database of known biometrics)?

A: No passengers are screened for their biometrics at this point in time. The passports are screened based on lookouts and other types of alerts.

Q: If biometric systems are in place, does the host government know of any countermeasures that have been used or attempted to defeat biometric checkpoints?

A; Not applicable.

Q: What are the host government's policies on collecting the fingerprints of travelers coming into the country?

A: The GOI currently does not collect fingerprints of travelers entering the country.

Q: Which agency is responsible for the host government's fingerprint system?

A: The Ministry of Interior's National Police (Polizia di Stato). The specific office is the Scientific Police Service of the Central Anti-Crime Division of the National Police's Department of Public Safety.

Q: Are the fingerprint programs in place NIST, INT-I, EFTS, UK1 or RTID compliant?

A: GOI interlocutors were unable to provide a response to this question.

Q: Are the fingerprints collected as flats or rolled? Which agency collects the fingerprints?

A: The fingerprints are currently collected as rolled, but the Ministry of Interior, which collects the fingerprints, is investigating flat collection technology.

¶6. (SBU) Section E: Passports

Q: If the host government issues a machine-readable passport containing biometric information, does the host government share the public key required to read the biometric information with any other governments? If so, which governments?

A: The GOI issues machine-readable biometric e-passports with biometric data chips embedded within them. All governments can access the biometric data through the Basic Access Control mechanism.

Q: Does the host government issue replacement passports for full or limited validity (e.g. the time remaining on the

original passports, fixed validity for a replacement, etc.)?

A: In case of theft or loss, the GOI does not issue a replacement passport but will issue a new fully-valid biometric passport.

Q: Does the host government have special regulations/procedures for dealing with "habitual" losers of passports or bearers who have reported their passports stolen multiple times?

A: The GOI at present does not have procedures applicable to this situation; the decision on how best to deal with "habitual" losers is left to the individual law enforcement or judicial authority deciding the case.

Q: Are replacement passports of the same or different appearance and page length as regular passports (do they have something along the lines of our emergency partial duration passports)?

A: N/A (see above)

Q: Do emergency replacement passports contain the same or fewer biometric fields as regular-issue passports?

A: The GOI does not release emergency replacement passports, only expedited regular passports.

Q: Where applicable, has Post noticed any increase in the number of replacement or "clean" (i.e. no evidence of prior travel) passports used to apply for U.S. visas?

A: No.

Q: Are replacement passports assigned a characteristic number series or otherwise identified?

A: As previously noted, Italy does not allow for duplicate passports. New full-validity passports are assigned new numbers.

¶7. (SBU) Section F: Fraud Detection

Q: How robust is fraud detection and how actively are instances of fraud involving documents followed up?

A: New generation Italian travel documents are highly fraud-resistant and are designed to facilitate fraudulence detection. Fraudulent documents that are detected are followed up through Interpol channels.

Q: How are potentially fraudulently issued documents taken out of circulation, or made harder to use?

A: Such documents would be taken out of circulation and examined by the issuing authority and relevant law enforcement agencies with a view toward avoiding future cases of fraud.

¶8. (SBU) Section G: Privacy and Data Security

Q: What are the country's policies on records related to the questioning, detention or removal of individuals encountered at points of entry into the country? How are those records stored, and for how long?

A: Italy has implemented a legal Code ("the Code") on personal data protection which implements an EU Directive (No. 95/46/CE). Moreover, in signing the Schengen Agreement, Italy has also agreed to enact in its national code minimum EU-mandated protection measures (Convention No. 108 of 1/28/1981 and Recommendation R(87) 15 of 9/17/1987). Within this framework, all personal data collected, used and stored for judicial purposes or for the protection of public safety can be held as long as necessary to achieve the objectives for which the data was collected. Criminal code procedures on using and keeping data acquired within a criminal proceeding (including secrecy of the minutes of the

interrogations or other acts of investigation) have not been in any way modified or made inapplicable by laws relating to data privacy protection. The Schengen Information System (SIS), to which border police offices are connected, allows Schengen countries to share information regarding denied admissions to the EU. This information is kept in the SIS for three years and can be renewed.

Q: What are the country's restrictions on the collection or use of sensitive data?

A: In general, Italian governmental institutions can only process sensitive personal data when such data is indispensable for specific, authorized institutional tasks

provided by law. These regulations do not apply to treatment of data for judicial, public order, or security reasons; for prevention, investigation, or repression of crime; or for the protection of and the security of the state. The Ministry of Interior is prohibited from collecting information and data on citizens in relation to their race, religious beliefs, political opinions, or their adhesion to the principles of unions, cooperatives, assistance organizations, or cultural entities.

Q: Are there any laws relating to security features for government computer systems that hold personally identifying information?

A: Public entities holding personal data in information systems are subject to the same rules as those for any other form of data bank. All government data banks must observe a minimum level of protection through the adoption of specific minimum security measures that will reduce to the minimum possible extent the risks of illegal disclosure of personal data. These levels of protection are detailed in the law.

Q: What are the rules on an individual's ability to access data that homeland security agencies hold about them?

A: By law, individuals have the right to confirm that government institutions are or are not holding data on the individual, and if data is being held, the individual has the right to obtain the data in an intelligible format. The Code (referred to above) provides for some derogation from such rights when data is held for judicial, public order and safety; for prevention, investigation or repression of crimes; or for national security. When data is held for national security reasons, the provisions of the Code related to the individual's rights do not apply.

Q: Does a non-citizen/resident have the right to sue the government to obtain these types of data?

A: Non-citizens and non-residents have the same right to access government held data about them as Italian citizens or residents.

¶9. (SBU) Section H: Immigration Data Bases

Q: What computerized immigration databases are used to track entries and exits?

A: The GOI does not maintain a computerized immigration database for use in tracking entries and exits. As mentioned above, the National Police watchlist/database is the operative system.

Q: If immigration databases are available at some POEs, but not all, how does the host government decide which POEs will receive the tool?

A: Not applicable.

Q: What problems, if any, limit the effectiveness of the systems? For example, limited training, power brownouts, budgetary restraints, corruption, etc.?

A: Not applicable.

Q: How often are national immigration databases updated?

A: Not applicable.

¶10. (SBU) Section I: Watchlist and Information Sharing

Q: Is there a name-based watchlist system used to screen travelers at POEs?

A: As mentioned above, the Italian Ministry of Interior maintains a database/watchlist that includes names associated with criminal and terrorist activities. See also sections A and C above.

Q: What domestic sources of information populate the name-based watchlist, i.e. names of deported persons, terrorist lookouts, criminal wants/warrants?

A: This list uses domestically collected information as well as INTERPOL and Schengen information. See also sections A and C above.

Q: What international watchlists does the host government use for screening individuals, e.g. Interpol or TSA No Fly lists, UN, etc.?

A: Currently, the MOI recognizes the U.S. No FLY/selectee list.

Q: What bilateral/multilateral watchlist agreements exist between host government and its neighbors?

A: Italy shares its watchlist information with all other Schengen states.

¶11. (SBU) Section J: Biometrics

Q: Are biometric systems in place at ports of entry (air, land, sea)? If no, does host government have plans to install such a system?

A: Biometric systems are not yet in place for points of entry but Italy has plans to implement a biometric system in order to comply with the Schengen Agreement by the end of 2008. The model currently being developed is "Italdata SPAID500." By the end of 2008 it is likely that digital fingerprint systems will be in place at all points of entry. The Italian government is looking at an E-Passport reader called "3M-IT." The name of the program for the distribution and operation of this technology is SIF.

Q: If biometric systems are available at some POEs, but not all, how does the host government decide which POEs will receive the tool?

A: With the implementation of the SIF system, all offices of the Border Police will have biometric control capabilities. Integrated biometrics systems will be phased in starting with the international/high volume airports such as Rome/Fiumicino and Milan/Malpensa and then distributed to other airports.

Q: What biometric technologies, if any, does the host government use, i.e. fingerprint identification, facial recognition, iris recognition, hand geometry, retinal identification, DNA-based identification, keystroke dynamics, gait analysis? Are the systems ICAO compliant?

A: Italy uses the Automated Fingerprint Identification System, which is ICAO compliant.

Q: Does the host government issue a machine-readable passport containing biometric information? If e-Passports are issued, what biometric information is included on the document, i.e. fingerprint, iris, facial recognition, etc? If not, does host government plan to issue a biometric document in the future? When?

A: The GOI issues machine readable e-passports with an integrated biometric chip that contains the passport holder's digital photo image. By the end of 2008, data related to digital fingerprinting will likely also be included in the biometric chips of newly-issued passports as such data

becomes available in the new systems.

¶12. (C//NF) Section K: Identifying Appropriate Partners

Q: Department would appreciate post's assessment of whether host government would be an appropriate partner in data sharing. Considerations include whether host government watchlists may include political dissidents (as opposed or in addition to terrorists), and whether host governments would share or use U.S. watchlist data inappropriately, etc.

A: Post has already taken steps to enter into a formal data-sharing agreement with the GOI. CA/P/IP, L/CA, the Terrorist Center (TSC) and Embassy Rome drafted and cleared through the HSPD-6 Interagency Working Group an Aide Memoire between the United States and Italy that was signed on December 4, 2007. This is the first step in establishing an exchange of terrorist screening information with Italy pursuant to HSPD-6. Formal negotiations of the operational protocol will follow.

Q: Are there political realities which would preclude a country from entering into a formal data-sharing agreement with the U.S?

A: There are no political considerations which would preclude Italy from entering into a formal data-sharing agreement with the U.S.

Q: Is the host country's legal system sufficiently developed to adequately provide safeguards for the protection and nondisclosure of information?

A: Yes. Italy's legal system is sufficiently developed to adequately provide safeguards for the protection and nondisclosure of information.

Q: How much information sharing does the host country do internally? Is there a single consolidated database, for example? Do different ministries share information amongst themselves?

A: See sections A and C above.

Q: How does the country define terrorism? Are there legal statutes that do so?

A: Article 270 of the Italian Penal Code defines terrorism as the following: "Conduct, which, by its nature and from its context, may cause serious damage to a country or an international organization and which is done with the aim of intimidating the population or compelling public powers or an international organization to perform or abstain from performing any act, to destabilize or destroy fundamental political, constitutional, economic or social structures of a country or an international organization, or any other conduct defined as terrorism or carried out for the purpose of terrorism in conventions or other international legal regulations which legally bind Italy, is considered to be for the purposes of terrorism." The conventions that bind Italy are the UN Conventions on Terrorism and all EU Agreements on Terrorism.

SPOGLI